Department of INFORMATION TECHNOLOGY

Maryland Account Management Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

The Maryland Department of Information Technology (DoIT) is responsible for ensuring the confidentiality, integrity, and availability of Information Technology (IT) systems. Establishing and maintaining a current and accurate account management policy ensures access to the IT infrastructure is provided to only those individuals required to authenticate to the network to perform their assigned duties and roles.

This document establishes the DoIT account management policy and requires all agencies not under the direct management of DoIT to develop a process for documenting, managing, and maintaining all user and system accounts authenticating to the IT infrastructure (detailed in Section 4.0). The requirements set forth in this policy are established by the standards described in NIST SP 800-53R4, SP 800-14, SP 800-50, SP 800-118 (retired, but not superseded).

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 7.2: Identification & Authorization Control Requirements and 7.2.1: User Authentication & Password Requirements. This policy also supersedes any related policy regarding account management declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy applies to all agencies supported by, or under the policy authority of, the Maryland Department of Information Technology. Agencies maintaining any IT systems that require, or can be configured with, authentication shall incorporate processes and procedures to meet the minimum requirements set within this policy.

4.0 Policy

This policy establishes the minimum requirements to effectively manage user, service, system, and network administrator accounts while ensuring access to systems and information are restricted based on assigned roles or specific services.

#	Name	Requirement
A	Account Management Tool	An account management tool, such as Active Directory, will be used to process and manage user and service accounts.
B	Role Based Access	DoIT and subordinate agencies will use **role-based access control** to manage roles and determine level of access needed to perform the duties assigned to those roles. ▪ Identify information and system access based on agency need and role, e.g., agency finance and contract personnel require access to budget data. ▪ Determine privileged-user roles per administrative function, and design with **least privilege** in mind, e.g., network team personnel need access to switches and routers. ▪ Restrict service account access to allow ONLY the function required for that service account, e.g., a service account that creates back-ups requires access only to offload and store data to a backup device.
C	Individual Accounts	▪ All users will be issued a unique, individual account; no shared accounts will be used unless otherwise authorized and used solely for business purposes (service desk shared inbox). ▪ Network and system administrators will have a standard user account and another administrative account to use when performing specific functions requiring an elevated privilege.
D	Continuous monitoring	All accounts will be subject to monitoring and data will be logged for compliance and auditing purposes.
E	Account Auditing and Review	Accounts will be audited periodically to ensure policy compliance and to review access levels and account status. Account creations, deletions, and permission changes will be reviewed for possible network exploitation.

4.1 Approval Process

DoIT will develop and maintain a standard, automated, process for requesting new user accounts within the Enterprise. This process will ensure requests are routed through appropriate management for approval as well as to determine the new user's required system and information access based on agency and role. This process will also be used by managers to inform the service desk of users who transfer to other agencies or have terminated employment. This ensures status changes to accounts are properly recorded and up-to-date and will help mitigate possible attacks against or use of inactive accounts.

Agencies not under direct management of DoIT will ensure a process is in place to manage account requests and status changes consistent with requirements indicated within this section.

4.2 Account Management Procedures

A set of procedures detailing a standardized methodology for creating, deleting, disabling, and maintaining accounts within the DoIT Enterprise will be established and managed by an Enterprise **Account Manager**. Agencies under the policy authority but not directly managed by DoIT will designate an agency Account Manager to meet the requirements of this policy.

The Account Manager ensures that all accounts conform to these procedures and can be audited for information including, but not limited to, the required level of access, account creator, and the list of approvers.

Administrative accounts will be separate accounts for system or network administrators who require specific, elevated privileges to perform the functions of their administrative roles. Blanket or domain administration accounts will be avoided to reduce the scope of damage from any compromised account or insider threat.

Service accounts will be created to allow only the functionality or access required for their specific tasks. These accounts will be maintained as privileged accounts and restricted to administrative personnel who manage the service account, with passwords protected as confidential data.

All accounts must meet the minimum requirements listed below:

- A uniform schema will be used for account identification that will encompass measures to address similar users, e.g., agencies having more than one John Smith.
- Required fields will be identified to facilitate the determination of user location (such as building/room number and phone number), agency affiliation, employee affiliation (civilian, military, contractor, vendor), and position or role within the agency.
- Upon notice of employee termination, accounts must be disabled immediately as well as passwords and secret question answers changed to prevent the employee from accessing the network or systems and possibly causing harm or data loss.
- Accounts will be audited periodically to mitigate permission creep, this ensures no individual account has access to information the user does not need to know or permissions to systems or devices to which the user does not require access.

4.3 Minimum Authentication Requirements

System and network technical controls (such as **Windows Group Policy**) will be implemented to manage minimum requirements for accounts to authenticate to the network. The following controls will be implemented within the network:

#	**Name**	**Requirement**
A	Signed AUP	All users will sign and submit, initially and yearly, an Acceptable Use Form (see *Acceptable Use Policy*) before being issued an account or accessing the network. Users with additional privileged access (administrator accounts) will also sign and submit, initially and yearly, a Privileged User Agreement Form (see *Acceptable Use Policy*).
B	Password Length	All Maryland network systems will use passwords at least 14 characters long.
C	Password Complexity	Passwords will be required to have at least 2 capital letters, 2 lower case letters, 2 numbers, and 2 special characters (such as the shifted number bar; !@#$... etc.).
D	Password History	Technical policies will enforce a 24 password history before an old password can be reused.
E	Maximum Password Age	▪ User and Administrator accounts will be forced to change passwords every 90 days ▪ Service account passwords may be set to never expire but must be denied local logon

#	Name	Requirement
F	Minimum Password Age	Users will be unable to change a new password (other than an initial password reset) for 1 day.
G	Failed Attempt Lockout	After 5 consecutive failed logon attempts, the user account will be locked. Service desk personnel will be able to unlock the account.
H	Lockout Time Period	Accounts will be locked out for a minimum of 15 minutes before being unlocked automatically.
I	Inactive Accounts	Accounts that are inactive for more the 60 days will be disabled. New accounts that are not used within the first 30 days will be disabled.
J	Deleting Accounts	Accounts will be disabled for at least one year before being purged from the system, unless otherwise required by specific regulations or standards.

4.4 Auditing

The agency-designated Account Manager will coordinate with the Information System Security Manager (ISSM) to ensure compliance with this policy (see *Auditing and Compliance Policy*). All users will be accountable for their actions and behavior while using the Maryland State IT assets. All users will be required to read and understand the DoIT Acceptable Use Form (see *Acceptable Use Policy*) before account issuance and as part of a yearly training and awareness campaign thereafter (see Section 4.5). A Privileged User Agreement Form (see *Acceptable Use Policy*) will be read and acknowledged by any user receiving privileged user account (administrator account) and as part of a yearly training and awareness campaign thereafter (see Section 4.5).

Users will be required to protect their accounts and must create secure, unique passwords. Agencies will audit user accounts periodically for weak passwords and review account inactivity to identify accounts exceeding the threshold indicated in section 4.3(I).

A consent-to-monitoring banner will be displayed on all systems, and users must accept monitoring before authenticating to the system. For onboarded agencies, user Internet behavior and system interaction will be logged and monitored by the DoIT Security Operations Center (SOC) to ensure compliance with policies and to prevent possible exploitation by external or internal threats (see *Continuous Monitoring Policy*).

4.5 Cybersecurity Awareness and Training

As part of the onboarding process, new users will:

- Receive training in proper system use
- Be informed of the processes and procedures for handling confidential data, e.g., MD sensitive data, PHI, and PII
- Understand current cybersecurity threats and their potential exposure, e.g., social engineering, malicious code, and inadvertent information exposure.

While much of the training of specific job functions will be handled by the new user's respective agency and division, technical training on properly accessing the systems and information security awareness helps ensure consistent use or best practices and standard operating procedures. Cybersecurity training and awareness will be implemented according to the requirements in the table below.

#	Name	Requirement
A	End User Support Team	Provide standardized system training to new users to ensure familiarity with system interactions, account information, support access, and location of common assets, such as printers, share folders and home directories.
B	Acceptable Use Form	Ensure users acknowledge and submit a signed Acceptable Use Form upon onboarding and yearly thereafter. Ensure privilege users, additionally, acknowledge and submit a signed Privileged User Agreement Form upon onboarding and yearly thereafter.
C	Information Security Awareness Training	Auditing and Compliance team provides a small binder of required information security awareness for new users to review before submitting the Acceptable Use Form.
D	Yearly Information Security Awareness Training	All users will be required to take yearly DoIT or State prescribed information security awareness training such as online tutorials, web-based training, or onsite training. Training will include, but is not limited to: ▪ Current social engineering threats ▪ Account protection ▪ Social media usage (personal responsibilities) ▪ Confidential information and how to protect nonpublic information ▪ Insider threat awareness and reporting responsibilities
E	Yearly Signed Acceptable Use Form	All users will be required to acknowledge and submit an Acceptable Use Form, and a Privileged User Agreement Form (where relevant) on a yearly basis. These forms will be recorded and maintained by the ISSM to ensure all users remain aware of the requirements for accessing and using State resources.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an agency under the policy authority of DoIT requires an exemption from this policy then that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Acceptable Use Policy
- Auditing and Compliance Policy
- Continuous Monitoring Policy

7.0 Definitions

Term	Definition
Account Manager	A system administrator role assigned to ensure the consistent and standardized creation, maintenance, and disposal of user accounts and user data on the network, including documenting established procedures, training other administrators in this process, and reviewing accounts for inaccuracies.
Least Privilege	The security objective of granting users only those access rights they need to perform their official duties.
Role Based Access Control	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.
Service Account	A special user account that an application or service uses to interact with the operating system.
Windows Group Policy	An infrastructure that allows implementation of specific configurations for users and computers, particular to the Microsoft Windows environment.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for managing and protecting Enterprise on-boarded agencies. DoIT will maintain access accounts according to established requirements authorized in the DoIT Cybersecurity Program Policy and described in this policy’s Section 4.0. Agencies not directly managed by DoIT must execute due diligence and due care to comply with the minimum standards identified within this policy

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency’s window of resolution or authorize DoIT to shutdown external and internal network connectivity until such time the agency becomes compliant.

Any attempt by personnel to circumvent or otherwise bypass this account management policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written notice, suspension, termination, or possibly criminal and/or civil penalties.